Homework VI (due April 21), Math 603, Spring 2003. (GJZ)

B I(a). Let k be a field of characteristic 0 and let $f(X) \in k[X]$ be an irreducible polynomial of degree $n \geq 2$. Write $\alpha_1, \ldots, \alpha_n$ for a full set of roots of $f(X)$ in its splitting field, M. We proved in class that M is normal over k, and as a corollary, this implies that for any two distinct roots α, β of $f(X)$, there is a k-automorphism, σ, of M so that $\sigma(\alpha) = \beta$. As every permutation is a product of transpositions, we deduce that for every permutation, π, of the roots $\alpha_1, \ldots, \alpha_n$, there is a k-automorphism, σ, of M so that $\sigma(\alpha_i) = \sigma(\alpha_{\pi(i)})$, for $i = 1, \ldots, n$. Consequently, if some difference of roots, say $\alpha_2 - \alpha_1$ is in k, by applying the k-automorphism, σ_j, so that $\sigma_j(\alpha_2) = \alpha_j$ and $\sigma(\alpha_i) = \alpha_i$ for all $i \neq 2$, with $j \geq 3$, we see that $\alpha_j - \alpha_1 \in k$ for $j = 2, \ldots, n$. Then, the sum of these differences is

$$\sum_{j=2}^{n} \alpha_j - (n-1)\alpha_1 = \sum_{j=1}^{n} \alpha_j - n\alpha_1 \in k.$$

But, $\sum_{j=1}^{n} \alpha_j$ is $\pm$ the coefficient of the term of degre $n-1$ in $f(X)$, thus in k, and since $\mathrm{char}(k) = 0$, we can divide by n, and we deduce that $\alpha_1 \in k$, which is absurd, as $f(X)$ is irreducible over k.

Now, for a counter-example if $\mathrm{char}(k) = p > 0$. We claim that the polynomial

$$f(X) = X^p - X - 1$$

over $k = \mathbb{Z}/p\mathbb{Z}$ is irreducible and has distinct roots, $\alpha_1 = \alpha, \alpha_2 = \alpha + 1, \ldots, \alpha_p = \alpha + p - 1$, where α is any of the roots of $f(X)$ in its splitting field, Ω. Since p is a prime, we know that

$$a^p = a, \quad \text{for every } a \in \mathbb{Z}/p\mathbb{Z}$$

and so

$$a^p - a - 1 = a - a - 1 = -1, \quad \text{for every } a \in \mathbb{Z}/p\mathbb{Z},$$

which shows that $f(X)$ has no root in $\mathbb{Z}/p\mathbb{Z}$. Thus, $\alpha \notin \mathbb{Z}/p\mathbb{Z}$. We also know that $(x+y)^p = x^p + z^p$, and so, for every $a \in \mathbb{Z}/p\mathbb{Z}$ (with $a \neq 0$)

$$f(\alpha + a) = (\alpha + a)^p - (\alpha + a) - 1 = \alpha^p + a^p - \alpha - a - 1 = 0,$$

since $\alpha^p - \alpha - 1 = 0$ and $a^p = a$, for all $a \in \mathbb{Z}/p\mathbb{Z}$. It remains to show that $f(X) = X^p - X - 1$ is irreducible over $\mathbb{Z}/p\mathbb{Z}$. Now, if $f(X)$ is reducible it can be factored as $f(X) = g(X)h(X)$, with $\deg(g), \deg(h) \geq 1$. If $\deg(g) = 1$, then $g(X)$ is of the form $X - \xi$, where $\xi \in \mathbb{Z}/p\mathbb{Z}$ is some root of $f(X)$, contradicting the fact that no root of $f(X)$ is in $\mathbb{Z}/p\mathbb{Z}$. So, we may assume that $2 \leq \deg(g) \leq p - 1$. In the splitting field, Ω, of $f(X)$, the roots of $g(X)$ are $\xi + i_1, \ldots, \xi + i_r$, where $r = \deg(g)$, $0 \leq i_j \leq p - 1$ and $\xi \in \Omega$ is some root of $f(X)$ not in $\mathbb{Z}/p\mathbb{Z}$. However,

$$\sum_{j=1}^{r} (\xi + i_j) = r\xi + \sum_{j=1}^{r} i_j$$

is equal to $\pm$ the coefficient of X^{r-1} in $g(X)$; this implies that $r\xi \in \mathbb{Z}/p\mathbb{Z}$, and since $2 \leq r \leq p-1$, we deduce that $\xi \in \mathbb{Z}/p\mathbb{Z}$, a contradiction. Therefore, $f(X)$ is irreducible over $\mathbb{Z}/p\mathbb{Z}$.

B II. Let $k \subseteq K$ be two fields of characteristic 0 and assume the following conditions:

(i) Every $f(X) \in k[X]$ of odd degree has a root in K.

(ii) For every $\alpha \in K$, the polynomial $X^2 - \alpha$ has a root in K.

(a) Let $g(X) \in k[X]$ be any polynomial of degree $\deg(g) = n \geq 1$. We prove by induction on m, where $n = 2^m n_0$ (with n_0 odd), that $g(X)$ has a root in K. The case $m = 0$ holds by (i), since n_0 is odd.

Assume that the induction hypothesis holds up to $m-1$, for any given $m \geq 1$. Let $\alpha_1, \ldots, \alpha_n$ be the roots of g is a splitting field, Ω, of g, and for any $r \in k$, let $\gamma_{ij}^{(r)} = \alpha_i + \alpha_j + r\alpha_i\alpha_j$, with $1 \leq i < j \leq n$. Let $h(X) \in \Omega[X]$ be given by

$$h(X) = \prod_{1 \leq i < j \leq n} (X - \gamma_{ij}^{(r)}).$$

We know that every coefficient, c_l, of $h(X)$ is $\pm$ some elementary symmetric function, s_l, in the indeterminates $\gamma_{ij}^{(r)}$, and so,

$$c_l = \pm s_l(\ldots, \gamma_{ij}^{(r)}, \ldots) = \pm s_l(\ldots, \alpha_i + \alpha_j + r\alpha_i\alpha_j, \ldots).$$

For every transposition $\pi = (i, k)$ of $\{1, \ldots, n\}$, if $j \neq k$, then $\pi(\gamma_{ij}^{(r)}) = \gamma_{jk}^{(r)}$, and if $j = k$, then $\pi(\gamma_{ij}^{(r)}) = \gamma_{ij}^{(r)}$. As every permutation is a product of transpositions, we deduce that c_l is a symmetric polynomial in $\alpha_1, \ldots, \alpha_n$. However, it is well-known that every symmetric poylynomial in $\alpha_1, \ldots, \alpha_n$ can be written as a polynomial in the elementary symmetric functions in $\alpha_1, \ldots, \alpha_n$. As these functions are $\pm$ the coefficients of $g(X)$, we have $c_l \in k$ for all l.

Moreover, $\deg(h) = n(n-1)/2 = 2^{m-1}n_0(2^m n_0 - 1) = 2^{m-1}n_0'$, where $n_0' = 2^m n_0 - 1$ is odd. Therefore, by the induction hypothesis, for every $r \in k$, there are some integers i_r, j_r with $1 \leq i_r < j_r \leq n$, so that $\gamma_{i_r j_r}^{(r)} \in K$ is a root of $h(X)$. Since $\mathrm{char}(k) = 0$, the field k must be infinite, and so, the set of pairs (i, j) as above is infinite. Note: Since $\mathrm{char}(k) = 0$, the field $\mathbb{Q}$ is contained in k, so, we may assume $r \in \mathbb{Z}$. This implies that there are $r_1 \neq r_2 \in k$ so that $i_{r_1} = i_{r_2} = i$ and $j_{r_1} = j_{r_2} = j$. Then,

$$\alpha_i + \alpha_j + r_1\alpha_i\alpha_j \in K \quad \text{and} \quad \alpha_i + \alpha_j + r_2\alpha_i\alpha_j \in K.$$

It follows that $\alpha_i + \alpha_j = \alpha \in K$ and $\alpha_i\alpha_j = \beta \in K$. Consequently, α_i and α_j are the roots of the quadratic equation

$$X^2 - \alpha X + \beta = 0.$$

Since $\mathrm{char}(K) = 0$, of course, this equation can be written as

$$(X - \alpha/2)^2 + \frac{4\beta - \alpha^2}{4} = 0.$$

We are reduced to proving that every element of K has a square root, but this is holds by (ii). Therefore, we conclude that $\alpha_i, \alpha_j \in K$, i.e., $f(X)$ has a root in K. It follows that every nonconstant polynomial $f(X) \in k[X]$ has all its roots in K.

BII (b) Further assume that K/k is normal of finite degree. Let $\mathcal{G} = \mathcal{G}(K/k)$ be the Galois group of K/k. As $\mathrm{char}(k) = 0$, we proved in class that the fixed field $\mathrm{Fix}(\mathcal{G}(K/k))$ is equal to k. If $g(X) \in K[X]$ is any polynomial of nonzero degree, let

$$h(X) = \prod_{\sigma \in \mathcal{G}} \sigma(g)(X).$$

Observe that h is fixed by all $\sigma \in \mathcal{G}$, so its coefficients are in $\mathrm{Fix}(\mathcal{G}(K/k)) = k$, and $h(X) \in k[X]$. By part (a), we know that $h(X)$ has some root $\theta \in K$. But, if $h(\theta) = 0$, then

$$\sigma(g)(\theta) = g(\sigma(\theta)) = 0,$$

for some $\sigma \in \mathcal{G}$, and thus, $\sigma(\theta)$ is a root of $g(X)$ in K. Therefore, K is algebraically closed.

BII (c) If $k = \mathbb{R}$ and $K = \mathbb{C}$, by the intermediate value theorem, (i) holds. If $\alpha \in \mathbb{C}$, we can write $\alpha = r(\cos\theta + i\sin\theta)$, where $r \in \mathbb{R}$ with $r \geq 0$. Then, $\sqrt{r}(\cos(\theta/2) + i\sin(\theta/2))$ is a square root of α. Moreover, $\mathbb{C} = \mathbb{R}[i]$ is a normal extension of degree 2, since i is a root of the irreducible (separable) polynomial X^2+1. By part (b), we deduce that $\mathbb{C}$ is algebraically closed.

BVI (a) Say k is a field with $\mathrm{char}(k) = p > 2$; let $K = k(X, Y)$ (where X, Y are indep. transcendentals over k) and let $f(Z) = Z^{2p} + XZ^p + Y \in K[Z]$.

First, observe that $f'(Z) = 2pZ^{2p-1} + pXZ^{p-1} \equiv 0$. Thus, $f(X)$ is inseparable over K. We claim that $f(Z)$ is irreducible in $K[Z]$.

If not, then either $f(Z) = (g(Z))^s$, where $g(Z)$ is irreducible, or $f(Z) = g(Z)h(Z)$, where $(g, h) = 1$ (with $g(Z), h(Z) \in K[Z]$). Since $f'(Z) = 0$, in the first case, $f(Z) = (g(Z))^s$, we get

$$sg(Z)g'(Z) = 0.$$

If p does not divide s, then $g'(Z) \equiv 0$. For degree reasons, we must have $g(Z) = Z^p + u$ and $s = 2$. Thus,

$$f(Z) = (Z^p + u)^2 = Z^{2p} + 2uZ^p + u^2 = Z^{2p} + XZ^p + Y \in K[Z]$$

which implies $2u = X$ and $u^2 = Z$. As X and Y are independent transcendentals over k, this is impossible. Thus, $p \mid s$, and for degree reasons, $s = 2p$ and $f(Z) = (Z^2 + aZ + b)^p$, where $a, b \in K$. It follows that

$$f(Z) = (Z^2 + aZ + b)^p = Z^{2p} + a^pZ^p + b^p = Z^{2p} + XZ^p + Y \in K[Z],$$

which implies that $a^p = X$ and $b^p = Y$ in $K = k(X, Y)$. However, this is impossible. Therefore, we are reduced to the case $f(Z) = g(Z)h(Z)$, where $(g, h) = 1$.

Since $f'(Z) = 0$, we get $g'h + gh' = 0$. Since $(g, h) = 1$, there exist $u, v \in K[Z]$ so that $ug + hv = 1$. Then, we have

$$g' = ugg' + g'hv = ugg' - gh'v = g(ug' - h'v).$$

If $g'(Z) \not\equiv 0$, then $g(Z)$ divides $g'(Z)$, which is absurd. Thus, $g'(Z) \equiv 0$. As $g'h + gh' = 0$, we also deduce that $h'(Z) = 0$. For degree reasons, we must have $g(Z) = Z^p + u$ and $h(Z) = Z^p + v$ (in $K[Z]$). Then,

$$f(X) = (Z^p + u)(Z^p + v) = Z^{2p} + (u + v)Z^p + uv = Z^{2p} + XZ^p + Y \in K[Z].$$

It follows that $u + v = X$ and $uv = Y$, which is impossible, as X and Y are independent transcendentals over k.

In conclusion, $f(Z)$ is irreducible over $K[Z]$.

Let $L = K(\theta)$, where θ is a root of $f(Z)$ in its splitting field. Assume that there is some $\beta \in L$ with $\beta \notin K$ and $\beta^p \in K$. If $f(Z)$ were irreducible over $K(\beta)[Z]$, then $f(Z)$ would be the minimum $K(\beta)$-polynomial of θ, and so $[L\colon K(\beta)] = 2p$. But, as $f(Z)$ is irreducible over $K[Z]$, we also have $[L\colon K] = 2p = \deg(f)$, and so, $K = K(\beta)$; this implies $\beta \in K$, a contradiction. Therefore, $f(Z)$ is reducible over $K(\beta)[Z]$.

We claim that $f(Z) = g(Z)^p$, for some $g(Z) \in K(\beta)[Z]$. If so, for degree reasons, $g(Z) = Z^2 + aZ + b$, and as we saw earlier, $X = a^p$ and $Y = b^p$, for some $a, b \in K(\beta) \subseteq L$. It follows that $X^{1/p}, Y^{1/p} \in K(\beta) \subseteq L$ and then

$$2p = [L\colon K] \geq [k(X^{1/p}, Y^{1/p})\colon K] = p^2,$$

i.e., $p(2-p) \geq 0$, but this is absurd, since $p \geq 3$.

Thus, it remains to prove that if $f(Z)$ is reducible in $K(\beta)[Z]$, then $f(Z) = (g(Z))^p$, for some $g(Z) \in K(\beta)[Z]$. The proof of the irreducibilty of $f(Z)$ in $K[Z]$ already proved that if $f(Z)$ is not a product of relatively prime factors, then $f(Z) = (g(Z))^p$. So, assume that $f(Z) = g(Z)h(Z)$, with $(g, h) = 1$. We already know from the proof of the irreducibilty of $f(Z)$ in $K[Z]$ that we must have $g(Z) = Z^p + u$ and $h(Z) = Z^p + v$, in $k(\beta)[Z]$. But now, as $f(\theta) = 0$, either $g(\theta) = 0$ or $h(\theta) = 0$. Say, $g(\theta) = 0$, the other case being similar.

Then, $\theta^p + u = 0$ with $u \in K(\beta)[Z]$, and since $\beta^p \in K$, we get $\theta^{p^2} \in K$. From $\theta^{2p} + X\theta^p + Y = 0$, we get

$$\theta^{2p^2} + X^p\theta^{p^2} + Y^p = 0.$$

If we write $\theta^{p^2} = a/b$, where $a, b \in k[X, Y]$, with $(a, b) = 1$, we get

$$a^2 + X^p ab + Y^p b^2 = 0.$$

Thus, $b \mid a$, and since $(a, b) = 1$, we may assume that $b = 1$. It follows that

$$a^2 = -(X^p a + Y^p),$$

which is impossible, as the degree of Y in a^2 must be even. Finally, this proves that L/K does not contain any purely separable element over K even though it is inseparable over K.

BVI (b) Let Ω be the a normal closure of L/K. We claim that $\mathcal{G}(\Omega/K) = \mathbb{Z}/2\mathbb{Z}$. This is because

$$Z^{2p} + XZ^p + Y = 0$$

has two distinct roots in Ω, each with multiplicity p. Indeed, if we let $U = Z^p$, then U is a root of $Z^2 + XZ + Y = 0$, which has two distinct roots, θ_1, θ_2, if $\mathrm{char}(k) = p \geq 3$. Then, we need to solve for $Z^p = \theta_i$, with $i = 1, 2$. Each of these equations has p multiple roots.

B VIII (a) Assume that K/k is a finite extension of fields and assume that K/k is separable. If so, $K = k(\theta)$, where θ is some root of some irreducible separable polynomial $f(X) \in k[X]$ and

$$K \cong k[X](f(X)).$$

In any extension L/k, we can write $f(X) = \prod_{i=1}^{t} g_i(X)$, where the $g_i(X)$ are mutually distinct irreducible polynomials, because $f(X)$ has distinct roots in its splitting field. Then,

$$K \otimes_k L = (k[X]/(f(X))) \otimes_k L \cong L[X]/(f(X)L) \cong \prod_{i=1}^{t} L[X]/(g_i(X)L).$$

However, as each $g_i(X)$ is irreducible over k, each $K_i = L[X]/(g_i(X)L)$ is a field. Moreover, each extension K_i/L is separable. This yields (1) $\Rightarrow$ (2).

Obviously, (2) $\Rightarrow$ (3).